FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

LIST OF REFERENCES CITED BY APPLICANT

(Use several sheets if necessary)

ATTORNEY DOCKET NO.	APPLICATION NO.
1573.1010	10/028,265
FIRST NAMED INVENTOR	
Koichi ITO, et al.	
FILING DATE	GROUP ART UNIT
December 28, 2001	

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
	AA						
	AB						
	AC						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO
TMS	AD	2000-305453	11/2000	Japan	—	—	X	
	AE	WO 99/67919	12/1999	WIPO	—	—	X	
	AF	WO 00/46953	08/2000	WIPO	—	—	X	
	AG	WO 00/27068	05/2000	WIPO	—	—	X	
	AH	WO 00/49765	08/2000	WIPO	—	—	X	
	AI	WO 01/10077	02/2001	WIPO	—	—	X	

OTHER REFERENCES *(Including Author, Title, Date, Pertinent Pages, Etc.)*

TMS	AJ	Kocker, Paul, et al., "Differential Power Analysis" in Proceedings of Advances in Cryptology-CRYPTO '99, Springer-Verlag 1999. pages 388-397.
	AK	Messerges, Thomas, et al., "Power Analysis Attacks of Modular Exponentiation in Smartcards", Cryptographic Hardware and Embedded Systems (CHES '99), Springer-Verlag, pages 144-157
	AL	Akkar, Mehdi-Laurent, et al., "Power Analysis, What is Now Possible...", ASIACRYPT 2000, Pages 489-502.
	AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", Proceedings of Fast Software Encryption Workshop 2000, Springer-Verlag, April 2000, which is called "a masking method."

EXAMINER	DATE CONSIDERED
	10/4/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NO. 1573.1010	APPLICATION NO. 10/028,265
LIST OF REFERENCES CITED BY APPLICANT		FIRST NAMED INVENTOR Koichi ITO, et al.	
(Use several sheets if necessary)		FILING DATE December 28, 2001	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
	BA						
	BB						
	BC						
	BD						
	BE						
	BF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO
TMS	BG	WO 00/24155	04/2000	WIPO	—	—	X	
TMS	BH	WO 00/24156	04/2000	WIPO	—	—	X	
	BI							
	BJ							
	BK							
	BL							

OTHER REFERENCES *(Including Author, Title, Date, Pertinent Pages, Etc.)*

TMS	BM	Messerges, Thomas S. et al., "Investigations of Power Analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, March 1999.
|	BN	Chari, Suresh, et al., "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Second Advanced Encryption Standard Candidate Conference, March 1999.
|	BO	FIPS 46, "Data Encryption Standard" Federal Information Processing Standards Publication 46, U.S. Departement of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VA, 1977.
↓	BP	http://csrc.nist.gove/encryption/aes/rijndael/Rijndael.pdf (which is linked from http://www.nist.gov/aes/).

EXAMINER	DATE CONSIDERED
	10/4/05

*EXAMINER: Initial if reference considered. whether or not citation is in conformance with MPEP 609: Draw line through citation if

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NO.	APPLICATION NO.
LIST OF REFERENCES CITED BY APPLICANT	1573.1010	10/028,265
	FIRST NAMED INVENTOR: Koichi ITO, et al.	
(Use several sheets if necessary)	FILING DATE: December 28, 2001	GROUP ART UNIT: 2131

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE
	AA	5,452,358	09/1995	Normile et al.			
	AB						
	AC						
	AD						
	AE						
	AF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO
TMS	AG	0 981 223 A2	02/2000	European Patent Office	—	~		
TMS	AH	0 792 041 A2	08/1997	European Patent Office	—	~		
	AI							
	AJ							
	AK							
	AL							

OTHER REFERENCES **(Including Author, Title, Date, Pertinent Pages, Etc.)**			TRANSLATION YES	TRANSLATION NO
TMS	AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", PROCEEDINGS OF FAST SOFTWARE ENCRYPTION WORKSHOP 2000, April 10-20, 2000, pages 150-164.		

EXAMINER	DATE CONSIDERED
	10/4/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.